HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

June 12, 2017

Guidelines on Data Export Security Assessments

David TANG | Min ZHU

On May 27, 2017, the National Standardization Technical Committee for Information Security ("**Technical Committee**") promulgated a draft for comment of the *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft)* (the "**Guidelines**"), in order to supplement the personal information and important data export assessment requirements stipulated under Cybersecurity Law, which came into force on June 1, 2017.

The Technical Committee, which is subordinate to the National Standardization Management Committee, is in charge of state information security standardization work under the guidance of the Office of the Central Leading Group for Cyberspace Affairs. Although the assessment standards referred in the Guidelines are not mandatory and are intended only for reference purposes, we believe these standards may reflect the attitude of regulators to some extent and therefore may provide practical guidance related to data export security assessments, particularly since the Cybersecurity Law and the forthcoming *Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (Draft)* (the "**Measures**") leave open questions as to personal information and important data export security assessments.

Relationship between the Guidelines and the Measures

The Measures are currently closed to further public comment. If practical, we expect that the Measures will be promulgated as soon as possible after only one round of comments (similar to the *Measures on Network Product and Service Security Reviews (Trial)*), in order to support the implementation of the Cybersecurity Law. However, as mentioned in a previous article, the Measures only contain general principles and standards. Detailed rules must still be developed to assist with its implementation. Thus, the Guidelines have been formulated to be consistent with the logical framework of the Measures, and contain more detailed requirements relating to data export security assessments.

For example, the Measures provide that personal information and important data export security assessments will involve either self-assessment by network operators or to assessments organized by industry regulators or supervisory departments depending upon specific circumstances. The Guidelines further provide in Part 4, "Assessment Procedures," the process and requirements for the security assessments to be conducted by network operators and clearly state that such processes and requirements may also apply to industry regulators or supervisory departments in preforming their regulatory duties.

In addition, Part 5 of the Guidelines, "Assessment Points," provides that two factors are to be considered for data export security assessments, which are the "legitimate and reasonable" and "controllable risk" related to the assessed data exports. Part 5 further explains the key assessment content as provided under Article 8 of the Measures. The Measures also provide that the specific scope of "important data" is to be determined by referring to the relevant national standards and important data identification guidelines. The Guidelines, as the recommended national standards developed by the Technical Committee, will certainly be consulted to determine the scope of important data, particularly the attached Appendix A, *Guidelines on the Identification of Important Data*.

Points of Interest

With respect to the Guidelines in the current form, we believe the following details are worthy of special attention:

a. Scope of application

The Guidelines apply to network operators for conducting personal information and important data export security assessments. As with the Measures, the Guidelines do not limit the subjects responsible for data exports security assessments to critical information infrastructure ("**CII**") operators. However, according to the remarks provided by a person in charge of Network Security Coordination Office of the Cyberspace Administration of China at a press conference immediately before the promulgation of the Cybersecurity Law, personal information and important data localization and export requirements are only to apply to CII operators rather than to all network operators. Thus, uncertainty continues to exist with respect to the application scope for the personal information and important data export security assessments. We look forward to clarification of the application scope in the formal issuance of the Measures.

b. Personal information

In addition to personal information that is defined under the Cybersecurity Law and the Measures, the Guidelines stipulate that an individual's location and behavioral information is also to be regarded as "personal information." This definition is consistent with the definition

of personal information as stipulated under the *Provisions on the Protection of Personal Information of Telecommunications and Internet Users,* which was promulgated prior to the Cybersecurity Law. This issue will require special attention from operators of smartphone apps which collect real-time user location information, especially apps that will provide services to users based upon collected real-time location information. App operators should observe that all location and behavioral information that they collect may be regarded as personal information under the Guidelines. Besides this, as the definition of personal information under the Cybersecurity Law is not exhaustive and the government tends to issue industry regulations that are more stringent, we further believe that personal information should be interpreted broadly and should include individuals' location and behavioral information.

c. Data exports and provision

The Guidelines clearly provide that "data exports" refers to the provision of personal information and important data that are in electronic form collected within the territory of People's Republic of China to foreign institutions or organizations. The provision of foreign data by Chinese institutions without any modification or processing is not regarded as data exports. In addition to network operators voluntarily providing or otherwise releasing domestic data to foreign institutions, users of products or services who provide data to overseas organizations, institutions or individuals through the products or services provided by the network operators are also to be regarded as data exports.

The Guidelines thus provide assurance to some network operators that not all form (including non-electronic forms) of personal information and important data that are provided to foreign institutions or individuals will be regarded as data exports. However, as the network operators providing personal information and important data to foreign entities through their users using their products and services are also identified as data exports, network operators may be subject to regulatory requirements if they intend to employ technical means or special transaction architecture to allow users to export data via their products or services.

d. Assessment procedures

In accordance with the Guidelines, the assessment procedures include commencing self-assessments, preparing assessment plans, evaluating assessment plans (legitimate and reasonable, and risk control) and developing assessment reports. Assessment reports are to be preserved for at least for five years and will undoubtedly become a necessary document for network operators' personal information and important data export security assessments. In light of the key assessment points as described below, preparing the assessment reports will require network operators to conduct comprehensive due diligence investigations on their network security and data protection status that are related to their business operations, including investigations into relevant technologies, laws and policies.

e. Key assessment points

As mentioned above, the factors necessary to be considered for data export security assessments mainly include the “legitimate and reasonable” and “risk control” for data exports. We understand that the “legitimate and reasonable” standard is relatively easy to prove. Network operators may prove this standard by demonstrating the data export is necessary for their business operations.

However, the "risk control” standard is relatively difficult to prove. The Guidelines provide that this standard is to be proven from the perspective of data attributes (personal information and important data), commercial subjects’ capacity (sender and receiver) and the stability of the macroeconomic environment (political and legal environment of the receiving party). Network operators may be subject to a heavy burden to prove this standard in this regard as a regulatory examination would be more comprehensive.

In addition, the Guidelines promote the “minimization principle” with respect to the assessment of personal information and important data to be exported. The minimization principle requires that the exported information and data must be directly related to the provider’s relevant business, which means that the provider’s relevant business processes cannot be fulfilled without exporting the information. The transmission frequency (automatic transmission) and quantity of information transmitted should be kept at the lowest frequency and the quantity necessary to fulfill the provider’s relevant business processes.

f. Appendix A: Important Data

Appendix A provides that the important data mentioned in the Guidelines refers to data (including original data and derived data) collected or developed by the Chinese government, enterprises and individuals within the territory of China, which do not involve state secrets but are closely related to national security, economic development and the public interest, and which if disclosed, lost, misused, tampered with or destroyed, or combined, integrated or analyzed without authorization, would cause severe adverse influences on national security, state economic and financial security, social and public interests or individual legal rights and interests.

In addition, Appendix A provides the scope of important data for 27 sectors (industries) for reference purposes, which essentially covers all major industry sectors and greatly exceeds the number of CII industries provided in the Cybersecurity Law. Appendix A concludes with a fallback provision that describes the standards for identifying important data in other industries which are not specifically provided for. Therefore, we tend to believe that the application scope of domestic data storage and export assessment should be interpreted broadly, provided that it does not prevent the orderly and free cross-border flow of data.

g. Appendix B: Assessment Measures

Appendix B of the Guidelines describes the assessment Measures in detail. First, the relevant network operators should assess the level of impact caused by personal information exports on individual rights and interests and the level of impact caused by important data on national security and social public interest, and should estimate the possibility of the occurrence of security event based upon sender and receiver's security capabilities and the local political environment of the location where the receiver is located. Secondly, network operators should make a comprehensive evaluation of the security risk related to the data export by considering the impact that the data exports may have on individual rights and interests, national security, and on the social public interest and the evaluation of the local political environment that the receiver is subject to and categorize the risk level as "extremely high," "high," "moderate" or "low." Data exports assessed as "extremely high" or "high" risk are to be prohibited.

Conclusion

The Guidelines provide detailed and practical requirements related to data export security assessments, which should be applied by different network operators on a case-by-case basis according to individual circumstances. Although the Measures and the Guidelines have not yet been formally introduced, the data localization and export assessment provided by the Cybersecurity Law will undoubtedly become a necessity. Therefore, we recommend that enterprises who may be subject to these requirements, whether or not they are CII operators, should make a preliminary assessment of their own circumstances in light of the Guidelines and prepare themselves in advance to respond to data export assessment requirements that may apply going forward.

Han Kun Cybersecurity and Data Compliance Series:

I : Big Data Policy and Legal Issues in the Healthcare Industry

II : Comments on the Network Security Law

III: Comments on the Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (for Public Comment)

IV: The Unveiling of Cybersecurity Reviews

V : Personal Information Protection from the Perspective of Criminal Law

● Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

Should you have any questions regarding this publication, please contact **Mr. David TANG （+8621-6080 0905; david.tang@hankunlaw.com ） or Mr. Min ZHU （ +8621-6080 0955; min.zhu@hankunlaw.com）.**